

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

KAJEET, INC.,

Plaintiff,

v.

TREND MICRO, INC.,

Defendant.

§
§
§
§
§
§
§
§
§

CIVIL ACTION NO. 6:21-cv-389-ADA

JURY TRIAL DEMANDED

PLAINTIFF'S BRIEF IN OPPOSITION
TO DEFENDANT'S MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

I. NATURE AND STAGE OF THE PROCEEDINGS1

II. SUMMARY OF THE ARGUMENT1

III. STATEMENT OF FACTS2

IV. LEGAL STANDARD.....4

V. ARGUMENT5

 A. Kajeet Sufficiently Pled Direct Infringement5

 B. Trend Micro User Guide Does Not Contradict Infringement Allegations.....8

 C. Asserted Claim Valid under 35 U.S.C. § 10113

 1. Kajeet has maintained consistent positions with respect to §10114

 2. Asserted claims valid in light of step two of the *Alice* inquiry15

 a. Claims directed to unconventional arrangement of components ..15

 D. Dismissal With Prejudice is Not Warranted18

VI. CONCLUSION.....19

CERTIFICATE OF SERVICE20

TABLE OF AUTHORITIES

Cases:

| | |
|--|-------------------|
| <i>Aatrix Software, Inc. v. Green Shades Software, Inc.</i> , 882 F.3d 1121 (Fed. Cir. 2018)..... | 16 |
| <i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)..... | 4, 5 |
| <i>BASCOM Glob. Internet Servs. v. AT&T Mobility LLC</i> , 827 F.3d 1341 (Fed. Cir. 2016)..... | 15, 16, 17, 18 |
| <i>Berkheimer v. HP Inc.</i> , 881 F.3d 1360 (Fed. Cir. 2018)..... | 16 |
| <i>Delavau, LLC v. Corbion NV</i> , 2016 U.S. Dist. LEXIS 78306 (D.N.J. June 15, 2016) | 8 |
| <i>Disc Disease Sols. Inc. v. VGH Sols., Inc.</i> , 888 F.3d 1256 (Fed. Cir. 2018)..... | 4, 5 |
| <i>Dr. Adekunle C. Omoyosi v. Texas Health & Human Services Commission</i> , 2021 U.S. Dist. LEXIS 122972 (S.D. Tex. June 14, 2021) | 19 |
| <i>Estech Sys. V. Regions Fin. Corp.</i> , No. 6:20-cv-00322-ADA, 2020 U.S. Dist. LEXIS 200484 (W.D. Tex. Oct. 28, 2020).. | 4-5 |
| <i>Ferguson v. Bank of N.Y. Mellon Corp.</i> , 802 F.3d 777 (5 th Cir. 2015) | 11 |
| <i>Finjan, Inc. v. Blue Coat Sys.</i> , 879 F.3d 1299 (Fed. Cir. 2018)..... | 16 |
| <i>Foman v. Davis</i> , 371 U.S. 178 (1962)..... | 18 |
| <i>Griffith v. Kroger Co.</i> , No. 9:05-CV-76-TH, 2008 U.S. Dist. LEXIS 131988 (E.D. Tex. Mar. 7, 2008)..... | 4 |
| <i>Kajeet, Inc. v. Gryphon Online Safety, Inc.</i> , 2021 U.S. Dist. LEXIS 37473 (D. Del. March 1, 2021)..... | 13-14, 15, 16, 19 |
| <i>Kajeet, Inc. v. Qustodio, LLC</i> , No. SA CV18-01519 JAK (PLAx), 2019 U.S. Dist. LEXIS 228067 (C.D. Cal. Nov. 1, 2019)..... | 13, 15, 16 |

| | |
|--|-------------------|
| <i>Lexington Luminance LLC v. Serv. Lighting & Elec. Supplies, Inc.</i> , No. 3:18-CV-01074-K, 2018 U.S. Dist. LEXIS 234331 (N.D. Tex. Oct. 9, 2018)..... | 5 |
| <i>Mayo</i> , 566 U.S. at 67..... | 16 |
| <i>Parity Networks, LLC v. Cisco Sys.</i> , 2019 U.S. Dist. LEXIS 144094 (W.D. Tex. July 26, 2019) | 4 |
| <i>Soar Tools, LLC v. Mesquite Oil Tools, Inc.</i> , No. 5:19-CV-243-H, 2020 U.S. Dist. LEXIS 166493 (N.D. Tex. Sep. 11, 2020) | 5 |
| <i>Tenehana Licensing LLC v. TigerConnect, Inc.</i> , 2020 U.S. Dist. LEXIS 183 (D. Del. Jan. 2, 2020)..... | 18-19 |
| <i>Vaporstream, Inc. v. Snap, Inc.</i> , Case No. 2:17-cv-00220-MLH, 2017 U.S. Dist. LEXIS 32884 (C.D. Cal. February 27, 2018) | 16 |
| <i>Waymark Corp. v. Porta Sys. Corp.</i> , 245 F.3d 1364 (Fed. Cir. 2001)..... | 7 |
| <u>Other:</u> | |
| 35 U.S.C. § 101..... | 2, 13, 14, 16, 18 |
| 35 U.S.C. § 271(a) | 7 |
| Fed. R. Civ. P. 15 | 18 |
| Rule 12(b)(6)..... | 4, 11 |
| Rule 15(a)..... | 18 |

I. NATURE AND STAGE OF THE PROCEEDINGS

Plaintiff Kajeet, Inc. (“Plaintiff” or “Kajeet”) files this Response to Trend Micro, Inc.’s (“Defendant” or “Trend Micro”) Motion to Dismiss Kajeet’s Original Complaint (“Motion”). For the following reasons, the Court should find that Kajeet’s Complaint sufficiently pleads infringement of U.S Patent No. 8,667,559 (“the ‘559 patent”) and deny Defendant’s Motion in its entirety.

II. SUMMARY OF THE ARGUMENT

Defendant contends that Kajeet has not met the pleading standards for direct infringement. But to do so would require holding Plaintiff to a higher standard than is required at the pleadings stage (where factual allegations must be taken as true), and imposing a higher degree of specificity than is required.

Kajeet’s Complaint and the allegations therein are sufficiently pled. The Complaint includes factual allegations identifying particular models of products that infringe at least one claim of the asserted patent – in particular, claim 27 of the ‘559 patent. Kajeet specifically names the Accused Products as all versions of the Trend Micro Premium Security Suite, Maximum Security, Internet Security, and Mobile Security products as well as any others that include Trend Micro’s parental control features. The Complaint also provides factual allegations describing the operation of the Accused Products, their structure and components, and which plausibly show how the accused products meet each and every limitation of the asserted claim. These allegations are based on information obtained from publicly available descriptions of the Accused Products authored by Defendant.

Kajeet’s Complaint undoubtedly includes more than enough information to provide Trend Micro with fair notice of Kajeet’s claims. Trend Micro effectively admits as much in its Motion,

stating that it understands Kajeet is asserting direct and indirect infringement of claim 27 of the ‘559 patent by the Accused Products. Motion at p. 2-3. Trend Micro further argues that statements in one of its user’s guides referenced in the Complaint contradict Kajeet’s infringement allegations and, therefore, Kajeet’s pleading is insufficient. However, Trend Micro has not shown how these particular statements conflict with Kajeet’s infringement theory or its long held positions on the scope of the claims.

As an alternative, Trend Micro suggests that the allegations in Kajeet’s Complaint are somehow different from arguments that it made in response to past challenges to the patent eligibility of the claims of the ‘559 patent rendering them patent ineligible. Yet, Kajeet has consistently taken the same positions in other courts and in its Complaint here with respect to the application of 35 U.S.C. § 101.

III. STATEMENT OF FACTS

Kajeet was founded in 2003 with the aim of developing solutions to an emerging technological problem - how to ensure safe operation of mobile communication devices by children and others. The known systems and methods for control prior to the time of the patented invention were largely inadequate and relied upon removing access to the communication device to prevent disallowed usage or utilized policy-based controls in which the policies were stored locally within accessible portions of the device’s memory. Policies are essentially rules that govern how and when users may utilize various functions of a mobile device. The prior systems were ineffective because the policies were locally accessible for manipulation or deletion. Kajeet addressed these shortcomings by storing usage policies remotely from the communication device(s). This arrangement improved operation of the systems through improved security from

user manipulation while accommodating real-time control of one or more devices which could be grouped to apply a set of policies to each simultaneously.

Kajeet's efforts and ingenuity have yielded thirty-eight U.S. Patents, many of which share a common specification to that of the asserted patents in this case. The Patents-in-Suit discuss how the proliferation of cell phones and other communication devices in modern life created the problem of providing adequate control over these devices, which typically accommodate a wide range of functionality accessible at any time from virtually anywhere.

Critically, the Patents-in-Suit note that prior art methods of controlling use of computing devices (*i.e.*, removing access by taking the device away or disabling it) were unworkable because they deprived the user of allowable uses of the device to prevent disallowed uses. The patents make clear that the problem to be solved is how to maintain effective control to prohibit certain uses while still allowing approved uses, all in the context of the user possessing the device at all times even when apart from or not in contact with the parent/administrator.

Kajeet's inventions provide access to desirable features, such as always allowing for calls to a parent, for example, while also preventing access to features deemed inappropriate because of cost (e.g., downloadable games or other applications), type of content (e.g., gambling or pornographic content), the time of day or night (e.g., during school hours or after bed time), and/or the device's location, among other criteria. The Patents-in-Suit disclose the use of policies defining acceptable and unacceptable uses of a mobile communication device based on a variety of contexts which are set by administrators (e.g., parents or teachers) at the server level to control use of one or more mobile communication devices. This represented an unconventional scheme that was neither well known nor routine for addressing a newly emerging problem in society. The inventions disclosed and claimed in the Patents-in-Suit provided for more robust control that was

more resilient to manipulation and/or disablement by users of the controlled devices and, therefore, more effective than prior art systems and methods.

IV. LEGAL STANDARD

To survive a motion to dismiss under Rule 12, “a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The court must construe the complaint in the light most favorable to the plaintiff, and determine whether the plaintiff may be entitled to relief under any reasonable reading of the complaint. *Parity Networks, LLC v. Cisco Sys.*, 2019 U.S. Dist. LEXIS 144094, at *2-3 (W.D. Tex. July 26, 2019). “A claim cannot be dismissed under Rule 12(b)(6) unless the plaintiff ‘would not be entitled to relief under any set of facts or any possibly theory that it could prove consistent with the allegations in the complaint.’” *Id.* (quoting *Griffith v. Kroger Co.*, No. 9:05-CV-76-TH, 2008 U.S. Dist. LEXIS 131988, at *2 (E.D. Tex. Mar. 7, 2008)). “In other words, it must appear beyond doubt that the plaintiff can prove no set of facts in support of their claim entitling them to relief.” *Id.* (citing *Griffith v. Kroger Co.*, No. 9:05-CV-76-TH, 2008 U.S. Dist. LEXIS 131988, at *2 (E.D. Tex. Mar. 7, 2008)).

The Federal Circuit has held that a complaint listing the asserted patents, specifically identifying accused products, and alleging that the accused products meet each and every element of at least one claim, is sufficient to meet the pleadings requirements under the plausibility standard of *Iqbal/Twombly*. *Disc Disease Sols. Inc. v. VGH Sols., Inc.*, 888 F.3d 1256, 1260 (Fed. Cir. 2018). District courts have interpreted *Twombly*, *Iqbal*, and *Disc Disease* to require a patent infringement Plaintiff to identify an accused product by name in most cases such that the Defendant is on notice of what specific conduct is alleged to constitute infringement.” *Estech Sys. v. Regions Fin. Corp.*, No. 6:20-cv-00322-ADA, 2020 U.S. Dist. LEXIS 200484, at *6 (W.D. Tex.

Oct. 28, 2020) (citing *Soar Tools, LLC v. Mesquite Oil Tools, Inc.*, No. 5:19-CV-243-H, 2020 U.S. Dist. LEXIS 166493, at *8 (N.D. Tex. Sep. 11, 2020)). “Additionally, the pleading standards established by *Twombly* and *Iqbal* require a plausible inference that an accused device meets all of the limitations of the asserted claims.” *Id.* (citing *Lexington Luminance LLC v. Serv. Lighting & Elec. Supplies, Inc.*, No. 3:18-CV-01074-K, 2018 U.S. Dist. LEXIS 234331, at *1 (N.D. Tex. Oct. 9, 2018)). “This cannot be inferred from bare conclusory allegations . . .” *Id.* at *6–7. “Additional factual information, at least pleaded on information and belief, that the accused devices practice the asserted claim is required.” *Id.* at *7. “However, this factual information does not necessarily need to be as detailed as that which will be disclosed in Plaintiff’s infringement contentions.” *Id.*

V. ARGUMENT

A. Kajeet Sufficiently Pled Direct Infringement

For the reasons set forth in the in the *Disc Disease* case, Kajeet’s Complaint includes sufficient allegations that the accused products meet each and every element of the asserted claims. *Disc Disease*, 888 F.3d at 1260. The Complaint clearly identifies the asserted patent and asserted claim. Specifically, the Complaint alleges infringement of claim 27 of the ‘559 patent. Dkt. 1, at ¶¶ 8, 39 (“Trend Micro’s quality testing and demonstrations of operation of the Accused Products to manage uses of computing devices directly infringe, either literally or under the doctrine of equivalents, at least claim 27 of the ‘559 Patent”); also attached as Dkt. 1, Exh. A.

The Accused Products of Trend Micro are also identified very clearly in the Complaint using the product names consistent with those presented on Trend Micro’s website and publicly available product literature. Dkt. 1 at ¶ 21 (“The Accused products of Trend Micro include all versions of the Trend Micro Premium Security Suite, Maximum Security, Internet Security, and

Mobile Security products as well as any others that include Trend Micro's parental control features); *see, also* Dkt. 1 at ¶¶ 20-26 (describing operation of identified Accused Products giving rise to infringement claims).

In its Complaint, Kajeet clearly alleges that the Accused Products meet each and every limitation of claim 27 of the '559 patent. Dkt. 1, at ¶ 39. The Complaint provides a thorough description of the structure and operation of the Accused Products addressing all of the components and operations that meet claim 27 as shown below:

[Preamble] 27. A method for controlling a computing device configured to execute a function using a communication network managed by a service provider, the method comprising:

The Complaint describes Trend Micro as a developer of software-based solutions accommodating feature management of (controlling) computing devices configured for operation on communication networks, including laptops, tablets, smartphones, and the like. Dkt 1., at ¶ 20. The communication network is described as being managed by a service provider, such as an internet service provider (ISP). *Id.* The Complaint also specifically identifies the Accused Products that meet the limitations of claim 27. Dkt 1., at ¶ 21.

[Element A] sending to a server a request to communicate with a remote computing device over the communication network;

In paragraph 23, the Complaint explains that local agent software (client software) is installed on the device and communications with software on Trend Micro servers to apply policy-based control of the device. Dkt 1., at ¶ 23. The Complaint also describes that the local agent software on the device effects this control by sending usage requests for communicating with other devices to Trend Micro serves for policy application. *Id.*

[Element B] receiving in real-time from the server a decision granting or denying the request, the decision based on a policy stored at the server and configured by an administrator; and

The policies for defining permissible or impermissible uses of the devices are set and stored

at the Trend Micro server by parents or administrators using the Trend Micro Mobile Security app. Dkt 1., at ¶ 24. The server applies the policies for the usage requests it receives and makes a decision about what devices features are usable or accessible by a particular device. *Id.*, at ¶ 25. The decisions based on the policies are communicated back to the managed device for enforcement. *Id.*, at ¶ 26.

[Element C] enforcing the decision by enabling a communication with the remote computing device over the communication network when the decision grants the request and by disabling the communication when the decision denies the request, the communication being enabled or disabled without storing the policy on the computing device.

The decision is enforced by local agent software on the controlled device by selectively permitting or blocking access to device features. Dkt 1., at ¶ 25, 26. The policies enforced on the device include controlling functions on the device to communicate with servers or other devices over the Internet. *Id.*, at ¶ 24. The policies are set and stored at the Trend Micro server by parents or administrators using the Trend Micro Mobile Security app without storing the policies on the devices themselves. *Id.*, at ¶ 24, 26.

Kajeet makes these allegations based upon its review of the publicly available product literature authored by Trend Micro describing its infringing products. The Complaint includes express allegations of Trend Micro's use of the method of claim 27 by 1) quality testing of the accused products, and 2) demonstrations of operation of the accused products.¹ *Id.* These allegations, which must be taken as true, are surely sufficient to put Trend Micro on notice of Kajeet's claims and the bases therefore.

¹ The Federal Circuit has long held that testing is a use of an invention which can give rise to liability for direct infringement under 35 U.S.C. § 271(a). *Waymark Corp. v. Porta Sys. Corp.*, 245 F.3d 1364, 1367 (Fed. Cir. 2001).

B. Trend Micro User Guide Does Not Contradict Infringement Allegations

Defendant's Motion is void of any argument or evidence competent to refute the allegations underpinning Plaintiff's claims of patent infringement. More specifically, Defendant presents no evidence whatsoever affirmatively showing either where policies are *stored* by the Accused Products or the processing steps and communications involved to *apply* those policies, which is what the asserted claims are directed toward. At best, the citations to the Product Guide proffered by Defendant show how a device is set up *prior to use with the Accused Products*, namely how to enroll a device and toggle on / select policies. They shed no light on where those policies are stored or how they are applied in operation, as discussed below.

Trend Micro asserts that its interpretation of the Product Guide is correct and completely discounts Kajeet's infringement allegations and the facts contained therein. Other courts have declined to grant a motion to dismiss even if the defendant contends the exhibits conflict with or contradict plaintiff's interpretations contained in its the infringement allegations.

If defendants' interpretation of the exhibits to plaintiff's complaint is correct, plaintiff may not ultimately prevail on its direct infringement claim. The Court, however, cannot credit defendants' interpretation of the exhibits over plaintiff's conflicting interpretation at this motion to dismiss stage. Consequently, plaintiff's direct infringement claim may proceed.

Delavau, LLC v. Corbion NV, 2016 U.S. Dist. LEXIS 78306, at *8 (D.N.J. June 15, 2016).

The entirety of Defendant's argument focuses on the storage location of policies implemented by the Accused Products. It is correct that the method of claim 27 of the '559 Patent requires a "decision [] based on a policy stored at the server." Plaintiff's Complaint recognizes this and presents plausible factual allegations showing how this limitation is met. Dkt. No. 1 at ¶¶ 23-26. Defendant's Motion does not contend otherwise. Rather, Defendant contends only that the factual allegations showing this limitation is satisfied cannot be true because they are purportedly

in direct conflict with the teachings of a Product Guide describing operation of one Accused Product.² Dkt. No. 8, at §IV.A (pp. 11-15). Stated another way, Defendant does not assert that, if taken as true, the allegations present in the Complaint are insufficient to show that all limitations of Claim 27 of the ‘559 Patent are met by the Accused Products. Defendant’s arguments go only to the plausibility of the allegations in light of the information presented in the Product Guide, which purportedly render the allegations of the Complaint implausible. Regardless, the Product Guide actually supports infringement.

First, Defendant presents portions of the Product Guide demonstrating how its software application is installed on the controlled device. Dkt. No. 8 at § II.C.1 (titled “Installation... on a Device”). The portions of the Product Guide highlighted therein provide instructions for downloading local agent software to the controlled device that perfectly align with allegations made in the Complaint. Dkt. No. 1 at ¶ 22 (“The Accused Products comprise a system of hardware (Trend Micro servers) and *software* (Trend Micro server software and the *local client software*) *implementable on computing devices*...”). As such, the Product Guide operates only to confirm the veracity of the allegations of the Complaint. Defendant further notes that these portions of the Product Guide are silent as to where policies for managing the device are stored. Dkt. No. 8 at p. 7.

² Excerpts from the Trend Micro Security 2021 for Windows Product Guide were attached as an Exhibit to the Complaint. Dkt. No. 1-3. This Product Guide is addressed to *a single implementation of one Accused Product*. Defendant agrees. Dkt. No. 8 at 6 (“the Product Guide describes... at least one Accused Product”). The Product Guide is wholly silent with respect to the several other implementations (on Android or iOS devices, e.g.) as well as to at least the Mobile Security products of Trend Micro, all of which are identified as Accused Products in the Complaint. Dkt. No. 1 at ¶¶ 21, 22. Therefore, the sufficiency of Plaintiff’s allegations with respect to these additional implementations and products is not at issue in deciding Defendant’s Motion.

Second, Defendant presents portions of the Product Guide demonstrating how “Parental Control feature[s]” are enabled. *Id.* at § II.C.2 (titled “Selection of the Parental Control Feature on the Device”). The screen shots and associated description within this section confirm that policies for “restrict[ing] a child’s access to certain activities or content” are set by administrators (i.e., parents) and show the steps taken to do so. *Id.* Again, this is entirely consistent with the allegations of the Complaint describing how policies are set by parents through the Trend Micro application to limit use of a child’s computing device(s). Dkt. No. 1 at ¶ 24.

Based on this alone, Defendant leaps to the unfounded conclusion that “all aspects of the Accused Products reside, function, and are configured locally on a managed device” and that “policies relating to parental controls are stored directly on the device.” Dkt. No. 8 at pp. 8, 10. Defendant provides no explanation of how installation of the software on the controlled device mandates these conclusions. The portions of the Product Guide to which Trend Micro cites do not address where the selected policies are stored or how they are applied following device setup. Where in the Product Guide is there a statement that the policies are stored on the device rather than on a Trend Micro server? There is not. All that is shown is that the device itself is used to access the Trend Micro interface for selecting policies that will subsequently be applied to control operation of that device. That is all. As such the Product Guide cannot contradict the allegations of the Complaint relating to the *location of policy storage* because it is silent on that, as Defendant recognizes.

It is immaterial whether the policies applied are *selected* using the device to be controlled or through another device. To be sure, claim 27 claims a method for controlling a device based on policies stored at a server, but does not set forth any specific requirements for how those policies are *selected* prior to effecting control over a computing device. *See* Dkt. No. 1-1 at claims.

Because no limitations requiring off-device policy selection exist, and because nothing in the Product Guide precludes storage of the policies upon which decisions are based be stored remotely on a Trend Micro server, as the Complaint alleges, the allegations of the Complaint must be taken as true and Defendant's Motion must be denied in its entirety.

Beyond this, additional information present in Product Guides relating to the Accused Products show that communication with a server is necessary to effect control over a computing device, thereby providing strong evidence supporting allegations that decisions are based on policies stored at Trend Micro's servers. For example, on iOS devices the Accused Products require a network connection and establishment of a VPN connection³ to Trend Micro's servers to operate⁴. See the excerpt below from the Product Guide for the iOS version of the Accused Products (i.e., iPhone, iPad). This iOS Product Guide is available at the same URL listed in paragraph 27 of the Complaint, and is attached as Exhibit 1 to the Vowell Declaration.

³ A VPN connection routes all network traffic through a designated communication path.

⁴ Materials that may be considered in deciding a Rule 12(b)(6) motion are limited to the contents of the challenged complaint and materials attached thereto. *Ferguson v. Bank of N.Y. Mellon Corp.*, 802 F.3d 777, 780 (5th Cir. 2015). However, certain exceptions exist and to the extent the Court considers additional portions of the Product Guide attached to Defendant's Motion beyond the excerpts attached to the Complaint, the embedded excerpts from another Product Guide for an Accused Product should likewise be considered.

VPN Settings

To turn on the VPN:

1. Tap the Web Guard panel in the Console. The VPN Off dial appears.
2. A popup indicates Web Guard needs permissions before you can use this feature. Tap the popup at the top to start the approval for permissions.



Figure 29. Web Guard



Figure 30. VPN Off

3. A popup dialog appears, indicating "Mobile Security" Would Like to Add VPN Configurations.
4. Tap Allow. Enter your device's password or use Touch ID to Add VPN Configurations.
5. The VPN turns On.



Figure 31. Add VPN Configurations



Figure 32. Enter Password or use Touch ID

6. Note the demo popup that remains. We'll show this later, so tap the X on the upper right of the popup to close it.

7. Tap VPN Settings to configure the settings. The VPN Settings screen appears, with two options.

RECOMMENDED VPN SETTINGS

8. Trend Micro Web Safe is pre-selected to allow ads and tracking, while blocking unwanted websites.

9. Trend Micro Parental Controls can be selected to protection your children.

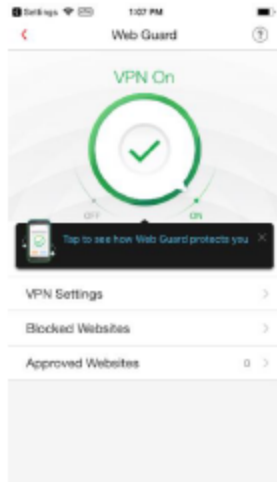


Figure 33. VPN On

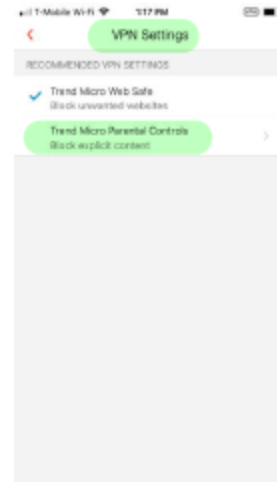


Figure 34. VPN Settings

Exh. 1, at p. 19-20.

The requirement for a VPN connection to Trend Micro servers to use its parental control features is consistent with the allegations of the Complaint relating to remote policy storage and decision making. As such, consideration of the Product Guides for the Accused Products tend to demonstrate the veracity of the allegations of the Complaint and certainly do nothing to preclude them from being accepted as true as the law requires.

C. Asserted Claim Valid under 35 U.S.C. §101

Two other district courts have declined to hold the asserted claims of U.S. Patent No. 8,667,559 (“the ‘559 patent”) invalid under 35 U.S.C. § 101. Those rulings came after extensive briefing on the issue from the parties as well as a § 101 Motion from another defendant in a related case. *See Kajeet, Inc. v. Qustodio, LLC*, No. SA CV18-01519 JAK (PLAx), 2019 U.S. Dist. LEXIS 228067, at *28 (C.D. Cal. Nov. 1, 2019); *Kajeet, Inc. v. Gryphon Online Safety, Inc.*, 2021

U.S. Dist. LEXIS 37473, at *21 (D. Del. March 1, 2021).

1. Kajeet has maintained consistent positions with respect to §101

Defendant contends that Kajeet has changed its positions with respect to the meaning of the asserted claims. Kajeet has been consistent in its description of the invention and its arguments for patent eligibility not only in this case but earlier litigations as well. Trend Micro's position relies primarily on its contention that it does not infringe the asserted claims. By this Motion, Trend Micro is effectively short circuiting the entire disclosure process for infringement contentions, invalidity contentions, and claim construction disclosures as set out in the Court's Order Governing Proceedings – Patent Cases.

As described above, Trend Micro incorrectly contends that Kajeet is attempting to cover products in which the policies are only stored on the local client devices rather than on a server. Trend Micro further asserts that Kajeet has changed the positions it took regarding patent eligibility which relied on remote storage of policies. One need look no further than the Complaint in this case to see that nothing Trend Micro's position is without merit. For example, the Complaint alleges the following:

“Other [prior art] solutions involving control through enforcement of decisions based upon policies defining permitted use that were set and stored only in accessible portions of the memory of the device itself, such as in the volatile memory of the device. These solutions were likewise ineffective as the policies upon which decisions effecting control were vulnerable to manipulation or deletion by virtue of their only being stored in accessible portions of memory of the computing device.” Dkt. 1, at ¶16.

The allegations in the complaint show that at all times Kajeet has correctly viewed the

asserted claims of the ‘559 Patent as requiring that policy decisions be ***based on*** policies stored remotely from the controlled device at a server. Trend Micro simply and improperly ignores the “based on” language present in the asserted claims.

Trend Micro also fails to recognize that the limitations present in the asserted claims do not go so far as to require that ***all*** policies may ***only*** be stored at the server. Indeed, Kajeet argued against this very construction in a prior case against the same counsel that now represents Trend Micro. *Kajeet, Inc. v. Qustodio, LLC*, 2019 U.S. Dist. LEXIS 228067, at *28 (*See* Tables at *17-18 and *27). In that case, the district court rejected the narrowing construction sought by the infringer while simultaneously denying a renewed *Alice* motion with respect to the same claim at issue in this case. In light of the allegations of the Complaint and the positions taken by Kajeet in this and prior cases, it is undisputed that there is no new news here that would impact patent eligibility. Kajeet has been consistent throughout in its description of the asserted claims and their scope.

2. Asserted claims valid in light of step two of the *Alice* inquiry

Trend Micro refers to the district court’s decision in the *Gryphon* case for its proposition that the asserted claims of the ‘559 patent are directed to an abstract idea. Motion, at p. 17. And while that court did make that finding, it ultimately denied Gryphon’s motion for patent ineligibility under §101 based on step two of the *Alice* analysis.

a. Claims directed to unconventional arrangement of components

Even if the claims of the ‘559 were directed to an abstract idea, they still introduce an inventive concept embodied in an unconventional arrangement of components as prescribed by the Federal Circuit. *See BASCOM Glob. Internet Servs. v. AT&T Mobility LLC*, 827 F.3d 1341, 1343 (Fed. Cir. 2016). The claims here describe a distributed architecture with policies stored

remotely from the device being managed – an arrangement that was not known or routine at the time. Dkt. 1, at ¶ 35. The district courts in the *Qustodio* and *Gryphon* cases agreed and followed the reasoning of the *BASCOM* case to deny the motion to dismiss on § 101 grounds. *Qustodio, LLC*, 2019 U.S. Dist. LEXIS 228067 at *45-47; *Kajeet, Inc. v. Gryphon Online Safety, Inc.*, 2021 U.S. Dist. LEXIS 37473, at *21 (D. Del. March 1, 2021).

For claims directed to a judicial exception under step one, courts are to “consider the elements of each claim both individually and ‘as an ordered combination’ to determine whether the additional elements ‘transform the nature of the claim’ into a patent-eligible application.” *Finjan, Inc. v. Blue Coat Sys.*, 879 F.3d, 1299, 1303 (Fed. Cir. 2018) (quoting *Mayo*, 566 U.S. at 67). The “inventive concept” must be something sufficient to ensure that the claims amount to “significantly more” than the abstract idea itself. *Id.* (quoting *Mayo*, 566 U.S. at 72-73). To satisfy this prong, the claims must include additional features which are significantly beyond “well understood, routine, conventional activity” or a simple “instruction to implement or apply the abstract idea on a computer.” *Mayo*, 566 U.S. at 79; *BASCOM*, 827 F.3d at 1349. Whether the claim elements or the claimed combination are well-understood, routine, or conventional is a question of fact. *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1128 (Fed. Cir. 2018).⁵ Courts have looked to the opinions of experts to aid in the determination of whether a claimed combination is well-understood, routine, or conventional. *Vaporstream, Inc. v. Snap, Inc.*, Case No. 2:17-cv-00220-MLH, 2017 U.S. Dist. LEXIS 32884 at *15 (C.D. Cal. February 27, 2018).

Kajeet’s Complaint incorporates the declaration of Dr. Knutson discussing the onset of the problem addressed by the Patent-in-Suit, prior art systems and methods for addressing it, and

⁵ See also *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018).

Kajeet's claimed solutions as expert evidentiary support for the well-pleaded factual allegations in the Complaint. *See* Dkt. 1, at p. 14, fn. 3; Exh. 2 to Vowell Declaration, at ¶¶ 16-22. The component arrangement required by the challenged claims, combined with remote policy storage in the context of feature management of a computing device, was not well-known, routine, or conventional and, further, its use effected an improvement in the operation of mobile communication device control systems. Dkt. 1 at ¶¶ 35-37; Exh. 2, at ¶¶ 29-30.

As described above and verified by Dr. Knutson, the claims of the Patent-in-Suit are directed to solving a problem arising from the rapid proliferation of mobile communications devices throughout society - a problem rooted in technology that requires a likewise technological solution. Dkt. 1, at ¶¶ 12-19. 34-37. Exh. 2, at ¶¶ 19-20. Means for preventing excessive or inappropriate use of such communication devices, which remain in the possession of children potentially all day and night, were needed. *Id.* The claimed inventions address this technology-centric problem by improving the security, effectiveness, and robustness of management of mobile devices. Dkt. 1, at ¶37. Exh. 2, at ¶ 24.

The Court here should follow the Federal Circuit's analysis in the *BASCOM* case where it reasoned that while "the limitations of the claims, taken individually, recite generic computer, network and Internet components, none of which is inventive by itself... an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces." *BASCOM*, 827 F.3d at 1349-50. The Court held the claims at issue were directed to patentable subject matter at step two because the record established that "the installation of a filtering tool at a specific location, *remote from the end-users*... cannot be said, as a matter of law, to have been conventional or generic." *Id.* at 1350 (emphasis added). It was the improved distributed architecture for an Internet content filtering system that the court found to be patent eligible subject

matter. *Id.*

Here, the challenged claims similarly require that the policies be stored remotely from the controlled device and with no less specificity than that provided in the claims of *BASCOM*. Further, the holding of *BASCOM* that the unconventional arrangement claimed was not well-understood, routine, or conventional at that time belies Defendant's assertion to the contrary.

D. Dismissal With Prejudice is Not Warranted

There simply is no basis for Trend Micro to seek a dismissal with prejudice given the record in this case. For the reasons stated above, Kajeet has sufficiently pled infringement. However, even if the Court determines otherwise, Plaintiff should be granted leave to amend its Complaint to address any specific issues.

Rule 15(a) provides that leave to amend "shall be freely given when justice so requires" Fed. R. Civ. P. 15. "In the absence of any apparent or declared reason - such as undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of the amendment, futility of amendment, etc. - the leave should, as the rules require, be 'freely given.'" *Foman v. Davis*, 371 U.S. 178, 182 (1962).

Here, Kajeet has not yet amended its pleading, and Trend Micro has pointed to no other legitimate reason for denying leave to amend. Trend Micro simply argues that leave should be denied for the same reason it contends the Complaint is insufficient, i.e., its assertion that the user guide contradicts Kajeet's infringement allegations.

The cases Trend Micro cites are distinguishable. The *Tenaha Licensing* case, the court granted the defendant's motion to dismiss based on patent ineligibility under 35 U.S.C. §101. *Tenehana Licensing LLC v. TigerConnect, Inc.*, 2020 U.S. Dist. LEXIS 183, at * 26. (D. Del. Jan

2, 2020). There, the dismissal was with prejudice because the plaintiff's argument about the specific improvements provided by the invention directly contradicted statements in the patent specification with respect to both steps one and two of the *Alice* analysis. There was no way for the plaintiff to amend its complaint in a manner that would render the asserted claims to be patent eligible subject matter. Further, in the other case cited by Trend Micro, the pro se plaintiff had amended his complaint twice, and the Court found that the plaintiff had not set forth facts that could plausibly support its causes of action. *Dr. Adekunle C. Omoyosi v. Texas Health & Human Services Commission*, 2021 U.S. Dist. LEXIS 122972, at * 15-16 (S.D. Tex. June 14, 2021).

Finally, Trend Micro references the *Gryphon* case filed by Kajeet in the District of Delaware. Trend Micro does not explain how the circumstances in that case provide any support for a dismissal with prejudice here. That case involved a different defendant with completely different products. There were, likewise, completely different infringement allegations made by Kajeet in that case. The district court in that case allowed Kajeet to amend its complaint, and then defendant Gryphon did not further challenge the sufficiency of the pleadings. *Kajeet, Inc. v. Gryphon Online Safety, Inc.*, 2021 U.S. Dist. LEXIS 37473, at *25. While a dismissal is not warranted here, Kajeet would respectfully seek leave of court to amend its complaint to address any issues the Court has with the Original Complaint.

VI. CONCLUSION

For the foregoing reasons, Kajeet respectfully requests that the Court deny Trend Micro's Motion in its Entirety.

Dated: July 19, 2021

Respectfully submitted,

/s/ Corby R. Vowell

Jonathan T. Suder

Michael T. Cooke

Corby R. Vowell

Richard A. Wojcio

FRIEDMAN, SUDER & COOKE

604 East 4th Street, Suite 200

Fort Worth, TX 76102

817-334-0400

Fax: 817-334-0401

jts@fsclaw.com

mtc@fsclaw.com

vowell@fsclaw.com

wojcio@fsclaw.com

ATTORNEYS FOR KAJEET, INC.

CERTIFICATE OF SERVICE

I hereby certify that on the 19th day of July, 2021, I electronically filed the foregoing document with the clerk of the court for the United States District Court, Western District of Texas, using the electronic case filing system of the court. The electronic case filing system sent a “Notice of Electronic Filing” to the attorneys of record who have consented in writing to accept this Notice as service of this document by electronic means.

/s/ Corby R. Vowell